

DRAFT

To: Agency Statewide Workgroup
From: The Office of HIPAA Implementation (OHI)
Date: October 22, 2001
Subject: HIPAA Assessment

Attached is a draft of the assessment tool, which OHI intends to use to fulfill the requirements of SB 456. OHI anticipates sending this assessment with a cover letter to each Department Director, and the Executive Officer of each Board, Program, and Commission.

The assessment package includes:

- The assessment tool,
- An appendix providing an overview of HIPAA, and
- An appendix listing the project steps for HIPAA compliance.

OHI is still working with the format; however, we believe the substance to be ready for review. We are interested in substantive comments by Friday, October 26, 2001, so that the final document can be released the following week.

Please provide your comments to Therese Hart via e-mail at: thart@chhs.ca.gov by Friday, close of business

Attachment:

**Health Insurance Portability and Accountability Act (HIPAA)
Office of HIPAA Implementation (OHI)**

HIPAA ASSESSMENT

Introduction This section explains why we have sent you this document, including the statutory requirement for this assessment, and how to use the document.

Purpose The objective of this assessment is to determine what programs in departments are covered by HIPAA regulations, and how HIPAA compliance impacts their operations. The document provides state departments with the information necessary to determine if HIPAA impacts your department's programs, business operations and systems, and requests feedback on that impact, and your department's current status of HIPAA compliance.

Background Federal Requirements

The Health Insurance Portability and Accountability Act (HIPAA), also known as the Archer/Kassebaum-Kennedy bill, became public law (P.L. 104-191) on August 21, 1996. HIPAA was introduced as a bill to improve the portability and continuity of health insurance coverage in group and individual markets; to combat waste, fraud and abuse in health insurance and health care delivery; to improve access to services and coverage; and to simplify the administration of health insurance.

HIPAA includes Administrative Simplification (AS) requirements intended to improve the efficiency and effectiveness of the entire health care system through the national standardization of electronic transactions and code sets. The HIPAA Privacy Rule establishes requirements for the handling of certain health care information to ensure privacy of patient health care data. Future AS rules will address unique health identifiers, security provisions, and enforcement.

The requirements apply specifically to entities considered to be a Health Plan, Healthcare Clearinghouse, Healthcare Provider, Business Associate or Trading Partner as defined by HIPAA. HIPAA will also impact departments that use, transmit, collect or report any of the information, which HIPAA covers under the Act.

State Law

Chapter 635, Statutes of 2001, creates the Office of HIPAA Implementation (OHI) in statute and enacts Section 130309 of the Health and Safety Code. Section 130309 requires all state entities subject to HIPAA to complete an assessment in a form specified by OHI, to determine the impact of HIPAA on their operations. Other state entities are also required to cooperate to determine

whether they are subject to HIPAA, including providing a completed assessment. OHI is required to report the findings of this assessment to the Legislature.

Instructions How to Use this Document

This assessment will help you determine whether you are covered by HIPAA requirements, and will provide OHI, the Administration, and the Legislature with an overview of which departments are affected by HIPAA, the extent of that impact, and the status of their compliance activities.

The definitions and examples provided here are accurate to the best of OHI's knowledge. This material should be viewed in the context of your own organization and environment. OHI encourages departments to obtain legal opinions or decision documentation if needed to apply or interpret HIPAA regulations.

Please fill out the assessment to the best of your ability, providing current estimates where final information may not be available.

The assessment should be returned to OHI by December 31, 2001 at:
Health and Human Services Agency
Office of HIPAA Implementation
1600 Ninth Street, Room 400
Sacramento, CA 95814

PART I

WHICH ORGANIZATIONAL CATEGORY BEST DESCRIBES YOUR DEPARTMENT?

Introduction This section helps you determine if you are a Covered Entity, and therefore, subject to HIPAA, or a Business Associate or Trading Partner of a Covered Entity or indirectly impacted. If you are not impacted by HIPAA, you can stop without completing the rest of the assessment.

Part I is intended to facilitate your department's determination of which organizational category best describes you. It will request that you evaluate your business processes, data collection and automated systems to make this determination.

Determine Health Information

First let's determine if your department has access to, or maintains *health information* as defined by HIPAA Regulations. The *health information* may reside in any medium (e.g., tape, paper, diskette, fax, e-mail, digital voice message). Below are examples of documents that may contain health information.

Definition

Health information is "any information, whether oral or recorded, in any form or medium that:

- 1) Is created or received by a healthcare provider, health plan, public health authority, employer, life insurer, school or university or healthcare clearinghouse in the normal course of business, and;
- 2) Relates to the past, present or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present or future payment for the provision of health care to an individual."


Examples:

Administrative	Education	Financial
<ul style="list-style-type: none"> - Cancer Registry - Certificates (Birth, Death, Other) 	<ul style="list-style-type: none"> - Behavior Rating Scales - Health Plan Records 	<ul style="list-style-type: none"> - Claims Information - Insurance Billing and Payment Information
Employee/Staff	Clinical	
<ul style="list-style-type: none"> - Disability Claims and Reports - Employee Assistance Program Information - Employee Health Records - Health Plan Enrollment Information - Worker's Compensation Claims & Reports 	<ul style="list-style-type: none"> - Complete Medical or Dental Files - Discharge Summary - Diagnosis Records - Doctor's Statements - Immunization Records - Laboratory Data - Medication Administration - Nursing Notes and Logs - Radiology Reports - Pathology Reports - Physician Orders - Psychological Records & Testing Reports - Treatment Plan - X-Ray Films 	

Decision

Does your department create, receive, send, maintain or have access to health information as described in the definition and examples above?

☐ Yes *Please continue with the assessment.*

☐ No  You do not need to proceed further with the assessment.

Please sign and return it according to the instructions above.



Determine Healthcare Provider

Second, let's determine if your department meets the HIPAA definition of a Healthcare Provider.

Definition

A *Healthcare provider* is "a provider of medical services including: *Institutional providers* (such as hospitals, skilled nursing facilities, home health agencies, comprehensive outpatient rehabilitation facilities); *facilities and practitioners* (including clinics and centers, physicians, clinical laboratories, pharmacies, nursing homes, licensed/certified healthcare practitioners and suppliers of durable medical equipment); and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business," related to the health of an individual.

Examples

Furnishes Healthcare Services	Bills for Healthcare Services	Is Paid for Healthcare Services
<ul style="list-style-type: none"> - Preventive - Diagnostic - Therapeutic - Rehabilitative - Maintenance - Palliative - Counseling - Physical/Mental Condition - Functional Status 	<ul style="list-style-type: none"> - Specific Healthcare - Sale/Dispense – Drug - Sale/Dispense – Device - Sale/Dispense – Equipment - Other Prescription Item 	<ul style="list-style-type: none"> - Procure Blood - Procure Organs - Procure Other Tissue - Contractual Services - Clinical Software - Ancillary Services

Decision

Does your department meet the definition of a Healthcare Provider by furnishing healthcare services, billing for healthcare services or receiving payment for healthcare services?

☐ Yes

☐ No

Please continue with the assessment.

Determine

Third, let's determine if your department transmits administrative or financial transactions, containing personally identifiable health information, electronically using the Internet, Intranet, private network system, magnetic tape or disk.

Examples

Administrative Transactions	Financial Transactions
<ul style="list-style-type: none"> - Enrollment/Dis-enrollment Health Plan - Referral Authorization for Services - Eligibility for a Health Plan 	<ul style="list-style-type: none"> - Coordination of Benefits - Health Claims - Health Claim Status - Healthcare Payment - Remittance Advice

Administrative Transactions cont'd.

- First Report of Injury

Financial Transactions cont'd.

- Healthcare Premium Payment
- Health Claims Attachments

Decision

If your department is considered a Healthcare Provider

And your department transmits administrative or financial transactions containing Personally Identifiable Health Information

Then your department is a Covered Entity under HIPAA Regulations.

Is your department a Covered Entity on the basis of the above?

☐ Yes

☐ No

Please continue with the assessment.

Determine**Health Plan**

Fourth, let's determine if your department meets the definition of a Health Plan.

Definition

Health plan means an individual or group plan that provides, or pays the cost of medical care.

Examples**Includes the following**

- An individual or group plan that provides or pays for the cost of medical care.
Has 50 or more participants
Is administered by an entity other than the employer
- Insured and self-insured plans
- An HMO (health insurance issuer)
- Part A or Part B Medicare
- Medicaid (Medi-Cal) Program
- Medicare + Choice Program
- Issuer of Medicare Supplemental policy
- Issuer of long term care policy, including a nursing home fixed indemnity policy
- Any arrangement that provides health benefits to the employee or 2 or more employers

Excludes the following

- Workers' compensation
- Automobile insurance carriers
- Government-funded program whose principle purpose is other than providing or paying the cost of health care (but do incidentally provide such services) e.g., WIC
- Government funded program e.g., government funded health centers and immunization programs
- Agencies that determine eligibility for enrollment in a health plan that is a government program providing public benefits, e.g., local welfare office.
- County Welfare Office exclusions (ask Terrie??)

Includes the following cont'd.

- Active military, Veterans Health Care Program, Civilian Health and Medical Program, Indian health service program, Federal Employees Health Benefit Plan
- An approved State child health plan
- A high risk pool that is a mechanism established under State law to provide health insurance coverage or comparable coverage to eligible individuals

Decision



Is your department considered an Individual or Group Plan that provides or pays for medical care according to the HIPAA definition? If so, it is a Covered Entity under HIPAA regulations.

Is your department a Covered Entity on the basis of the above?

☐ Yes

☐ No

Please continue with the assessment.

Determine

Healthcare Clearinghouse

Fifth, let's determine if your department meets the definition of a Healthcare Clearinghouse.

Definition

A Healthcare clearinghouse is a "private or public entity that processes or facilitates the process of health information received from another entity," either to or from the standard format that is required for electronic transactions.

Decision



Does your department receive or send health information from or to a Covered Entity, and process that information either to or from the standard format that will be required for administrative or financial electronic transactions?

☐ Yes

☐ No

Please continue with the assessment.

If your department processes health information received from a Covered Entity

And sends the information to another Covered Entity,

Then your department is a Covered Entity under HIPAA Regulations.

Are you a Covered Entity on the basis of the above?

___ Yes

___ No

Please continue with the assessment.

Determine Business Associate or Trading Partner

Now, let's determine if your department meets the HIPAA definition of a Business Associate or Trading Partner.

Definition

A *Business Associate* is a person or entity that performs a function or assists a Covered Entity with a function or activity involving the use or disclosure of Individually Identifiable Health Information (IIHI). Please note, a *Covered Entity* may be a *Business Associate* of another *Covered Entity*.

Individually Identifiable Health Information (IIHI) "is information that is a subset of health information, including demographic information collected from and individual and:

- 1) Is created or received by a healthcare provider, health plan, public health authority, employer, life insurer, school or university or healthcare clearinghouse and;
- 2) Relates to the past, present or future physical or mental health or condition of an individual; the provision of healthcare to an individual ; or the past, present or future payment for the provision of healthcare to an individual and identifies the individual; it is it believed the information can be used to identify the individual."

Examples

<ul style="list-style-type: none">- Claims processing or administration- Data analysis- Utilization review- Quality Assurance- Billing- Benefit management- Proactive management and repricing- Legal	<ul style="list-style-type: none">- Actuarial- Accounting- Consulting- Data aggregation- Management- Administration- Accreditation- Financial Services
--	---

Decision



Does your department perform a service or function on behalf of an entity that has been deemed to be a Covered Entity as defined by the HIPAA Regulations?

☐ Yes

☐ No

Please continue with the assessment.

If your department performs a service/function on behalf of a Covered Entity

Then your department is a Business Associate under HIPAA Regulations.

Are you a Business Associate?

☐ Yes

☐ No

Please continue with the assessment.

Definition

A *Trading Partner* is a person or organization that exchanges health information via electronic transmissions with a Covered Entity.

Decision



Does your department electronically exchange health information, as defined on page 2, with a Covered Entity?

☐ Yes

☐ No

If your department electronically exchanges health information with a Covered Entity via electronic transmissions

Then your department is considered a Trading Partner under HIPAA Regulations.

Are you a Trading Partner?

☐ Yes

☐ No

Please continue with the assessment.

Determine Data Content Impact

Now, let's determine if your department uses any codes or transactions that will be changed by HIPAA Regulations.

Definition

Data content includes any set of codes used to encode data elements, such as tables of terms, medical concepts, medical diagnostic codes, or medical procedure codes. A code set includes the codes and the descriptors of the codes.

Departments, counties, insurance carriers, and providers use health insurance code sets to bill, collect data and report with.

Decision



- 1) Does your department use health care procedure codes (e.g., Appendectomy, Chest X-Ray, Urinalysis) for any of its business functions?
- 2) Does your department use diagnosis codes (e.g., Appendicitis, Congestive Heart Failure, Urinary Tract Infection) for any of its business functions?
- 3) Does your department use drug/pharmacy codes (e.g., Penicillin, Claritin) for any of its business functions?
- 4) Does your department use dental codes (e.g., Tooth Extraction) for any of its business functions?

If your department uses, transmits, collects data or reports using any of the types of data noted above

Then your department may be impacted by data content changes from a Covered Entity, Business Associate or Trading Partner.

Will your department be impacted by Data Content changes?

___ Yes

___ No

Please continue with the assessment.

Summary

Based on these questions and answers, I have determined that my department is:



- ___ a Covered Entity
- ___ a Business Associate
- ___ a Trading Partner
- ___ impacted by Data Content changes
- ___ not covered by HIPAA

This concludes Part I of the Assessment.

If you are a Covered Entity, Business Associate, Trading Partner, or impacted by Data Content changes, please continue with Part II, and tell us more about how HIPAA impacts your department and how you are preparing for that impact. If you are not covered by HIPAA, please

indicate that above. You do not need to complete Part II. Please sign and return the form according to the instructions on page 2.

PART II

WHAT KIND OF IMPACT WILL HIPAA HAVE IN YOUR DEPARTMENT?

Introduction Now that you have reviewed your business processes and made determinations regarding the need for your department to be HIPAA compliant, we are interested in specific information regarding HIPAA's impact to you, and the status of your department's efforts.

Impact

1) The final Federal HIPAA rules that affect me are:

- ☐ Transactions and Code Sets
☐ Privacy

2) The programs within the department that are affected by HIPAA are

3) Please identify key organizations with whom you exchange health information (e.g., insurance companies, Providers, Medi-Cal, Counties)

Status

We are interested in the *status* of your efforts to address the HIPAA regulations.

1) What is the current status of your department's HIPAA efforts? The "Steps to HIPAA Compliance" document (Appendix A) will help you answer the HIPAA Compliance Steps questions.

☐ Not started yet

☐ Attending Statewide workgroup/Sub-workgroup meetings

HIPAA Compliance Steps	Completed this Step?	
Project Initiation (Awareness)	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Initial Assessment (Inventory)	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Project Plan	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Detailed Assessment (Gap analysis)	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Implementation	<input type="checkbox"/> Yes	<input type="checkbox"/> No

2) Have you identified a HIPAA coordinator?

If so, whom?

Name _____ Title _____

Phone _____ E-mail _____

3) Is any portion of your HIPAA work contracted out?

☐ Yes

If so, what portion? _____

What contractor? _____

☐ No _____

4) Have you established a Project Management Office? ☐ Yes ☐ No

5) Is there anything that you would consider unique in your project management strategy (e.g., Department-wide interdisciplinary teams)?

☐ No _____

☐ Yes, our department

6) Have you met with your Business Partners? ☐ Yes ☐ No

Whom? _____

7) Is someone in your Department assessing HIPAA impact to State laws and/or regulations and determining where changes are required? ☐ Yes ☐ No

8) Do you anticipate that you will be fully compliant by the Federal deadlines?

Rule:	Federal Deadline:	Meet Deadline?
Transactions & Code Sets	10/17/02	<input type="checkbox"/> Yes <input type="checkbox"/> No
Privacy	4/14/03	<input type="checkbox"/> Yes <input type="checkbox"/> No

If your department will not be fully compliant, please identify areas of non-compliance _____

9) Are you involved in any National Standards Organizations or Workgroups? Please identify

Scope

We are interested in the scope/size of HIPAA impact to your department.

1) Describe the HIPAA impact to your department relative to:

• Essential Services: _____

- Programs (identify programs (e.g., Medi-Cal) within your department that are affected by HIPAA):

- Business Partners/Stakeholders:

- Information Technology (IT) systems (identify the IT systems that will require remediation):

- Customer interfaces:

- 2) What are your department's major/specific HIPAA issues and challenges (e.g., Medi-Cal's elimination of thousands of local codes)? Please quantify.

Fiscal



- 1) Have you estimated the cost for HIPAA assessment and remediation (in total or by rule)?

If so, how much:

Transactions and Code Sets \$ _____

Privacy \$ _____

Total \$ _____

- 2) Over what period of time?

01 / 02 \$ _____

04 / 05 \$ _____

02 / 03 \$ _____

05 / 06 \$ _____

03 / 04 \$ _____

- 3) Have you estimated the cost for Project Management/contractor team? If so, how much? \$ _____

- 4) Over what period of time?
- | | |
|------------------|------------------|
| 01 / 02 \$ _____ | 04 / 05 \$ _____ |
| 02 / 03 \$ _____ | 05 / 06 \$ _____ |
| 03 / 04 \$ _____ | |
- 5) Is there any money in your department's base that you can use? If so, how much? \$ _____
- 6) Have you requested funding for the current year? If so, how much \$ _____
- 7) Have you received funding for the current year? If so, how much \$ _____
What is the status of your funding request? _____
- 8) Have you requested funding for the budget year? If so, how much \$ _____
What is the status of your funding request? _____
- 9) Do you anticipate requesting funding for the budget year at a later date? If so, please provide an estimate \$ _____
- 10) Please identify funding sources (e.g., special fund, federal fund) _____

Estimate funding proportions (e.g., 10% general fund, 90% federal funding)
\$ _____
- 11) Please identify any redirected resources _____

Department Deputy Director Signature

Date

Please return this Assessment by December 31, 2001 to:

Health and Human Services Agency
Office of HIPAA Implementation
1600 Ninth Street, Room 400
Sacramento, CA 95814

DRAFT -- HIPAA OVERVIEW

WHAT IS IT

The Health Insurance Portability and Accountability Act (HIPAA) will change certain aspects of the way health care is administered over the next few years. President Clinton signed the Archer/Kassebaum-Kennedy Health Insurance Portability and Accountability Act on August 21, 1996. HIPAA is designed to expand health coverage by improving the portability and continuity of health insurance coverage in group and individual markets; to combat waste in health care delivery; to promote the use of medical savings accounts; to improve access to long-term care services and coverage; and to simplify the administration of health insurance. Within this context, HIPAA includes a provision called Administrative Simplification, which is intended to improve the efficiency and effectiveness of the health care system by encouraging the development of standards for the electronic transmission of certain health information. HIPAA also establishes privacy and security standards related to health information.

NATIONAL STANDARDS

Through the adoption of national standards, the health care industry can realize cost savings by reducing administrative duplication. These standards are developed by processes delineated in the HIPAA legislation and are established by the publication of a "rule" in the Federal Register. There are currently eight proposed rules within the HIPAA legislation, more will likely follow in the next few years.

Once each rule is published in the Federal Register, following a 60 day Congressional concurrence period, organizations have 24 months to become compliant. Public agencies are not exempt from HIPAA and must comply with the law, which impacts Covered Entities, described by HIPAA as Providers, Clearinghouses and Health Plans. Programs within State Agencies that fund health care services, under HIPAA, are usually considered health plans.

The "Transaction and Code Sets" rule, published in August 2000, was the first rule published. Health care organizations have until October 16, 2002 to comply with its requirements. The Transaction and Code Sets rule will apply to those Covered Entities that perform the following business functions:

- send or receive health care claims
- pay health care services
- send or receive eligibility inquiries
- conduct provider referrals and service authorizations
- perform health plan enrollment
- perform coordination of benefits activities

The second rule is the Privacy Rule published in December 2000. Health care organizations have until April 14, 2003 to comply with its provisions. The Privacy Rule applies requirements for viewing, handling and storing patient identifiable health care information that is written, electronic, faxed, when present on a monitor screen, or verbal. It will require a review and possible revision of many information policies, procedures and practices.

WHO MIGHT BE IMPACTED

All public health and behavioral health programs will be impacted. Departments and program areas may be impacted to varying degrees, dependant upon the types of services they provide, their current administrative processes or if they handle certain health care information.

Any program area would almost certainly be impacted if it:

- *receives, submits or pays health care claims,*
- *is involved in plan enrollment or benefits, or*
- *receives, distributes or retains patient health care data.*

Any program may be impacted if it:

- *receives or submits medical information from / to a business partner,*
- *utilizes information collected from a provider working in a HIPAA compliant environment,*
- *uses detailed or summary medical information from other entities, or*
- *generates reports from medically related information.*

Health care and medical information will have new code set standards and formats. There are also new rules for the receiving, distributing and retaining of this information. Any departmental program involved in service delivery, collection, storage or distribution processes may be impacted. These programs need to review their business processes and automated systems for potential impact and identify actions to ensure compliance with the HIPAA Rules, as well as ensure essential services are not impacted. An important component is the communication and coordination with your business partners.

HIPAA will eliminate the use of "local codes", codes that are not within the standard code sets. These code sets include medical procedure, health care service, mental health services, and administrative reporting codes. Many such codes are utilized to support key programs within county and provider processes. Program areas will need to identify for new ways to track and report services currently supported by non-standard codes. If alternative reporting solutions are not developed, an entity's ability to administratively support some of its programs may be negatively impacted. All county and state programs that use local codes need to consider options for compliance. This will require coordination with business partners.

The Privacy Rule deals with health information that is individually identifiable. While all entities should have security and privacy policies in place, the HIPAA standards may be more stringent and may require documentation that is not currently in place today. Each program needs to review its policies to ensure compliance, and will need to provide education and training to every person (employee, contractor, and temporary help) that potentially has access to health care data. The federal deadline for compliance with the Privacy Rule is April 14, 2003.

Other examples of potential impacts to consider include:

- Our business partners may use HIPAA compliant data collection processes that have limited coding sets, new field attributes and new definitions from current practices. These data collection processes may not provide enough specificity to meet current program objectives. For example, race – ethnicity codes in the HIPAA required standard format do not use the range currently used by many of California's programs.
- There may be additional costs to collect and report non-HIPAA compliant data.
- The Provider Taxonomy proposed may not uniquely break out the various types of providers currently defined. Provider reports may be impacted.
- In future rules, Provider numbers will be established at a national level and may not resemble the currently used numbers. Having access to currently valid numbers will be important in service delivery, edits and audits.
- Access and storage of data and records need policies and procedures in place to ensure clients have access to their health information, the ability to exercise their right to note modifications to these records, and can obtain a history of releases of their health information.
- Data transmission with business partners may require additional processes. Contract language should require that business partners apply HIPAA compliant processes. Encryption and authentication processes may be needed when data is moved between business partners.
- Periodic audits of security, privacy and business practices may be needed to document that reasonable processes and procedures have been initiated to meet federal standards and minimize liabilities.
- Similar entities may wish to adopt similar policies and procedures to ensure consistent applications of the federal standards.
- Changes to policies, regulations, and legislation may be needed to ensure HIPAA compliance, and support revised data collection, reporting and information sharing processes and procedures.
- Programs that operate a health plan for employees or constituents have potential impacts.
- Programs that use provider numbers, diagnosis codes, drug codes, local codes, health plan codes, or pass data to business partners may be impacted. Information access will most probably be more restrictive than our present practices. This may also require new computerized access controls.

HIPAA COORDINATION WORKGROUP

The interdependence between state departments, counties, providers and program areas that perform health related service delivery or use health information makes it vital that we approach HIPAA with a unified voice and common methodology. There are many critical issues that are still outstanding and each department's view, as well as the opinion of their business associates, should be consistently expressed at both a local and a national level. In addition, with over 90,000 providers throughout California, it is imperative that we perform outreach, education and training in a manner that is efficient and well coordinated. Further, requests for resources must be coordinated and overall progress on implementation should be monitored and coordinated so issues can be addressed quickly.

With this in mind, a California Health and Human Services (CHHS) Agency Workgroup has been established to coordinate HIPAA compliance activities on a Statewide basis. The group has focused on awareness, issue identification and analysis, and tracking implementation efforts. Because of the need to coordinate and review HIPAA implementation, this workgroup is designated as the primary vehicle to move forward with HIPAA compliance for the CHHS Agency. It is suggested that representatives from each entity participate in the meetings and the various subject area sub-workgroups (e.g., Security/Privacy Sub-workgroup). It is critical that state and county issues are recognized, communication and coordination achieved, and a California voice be heard in national forums. For information on HIPAA and the Agency's Statewide Workgroup, please contact Ken McKinstry, at Kmckinst@dmhhq.state.ca.us.

ACTION IS NEEDED NOW

Action is needed now to ensure compliance with HIPAA rules within the federal timelines. State entities and Counties may need to form workgroups to raise awareness, assess impacts, implement changes, address issues and coordinate with business partners as their programs, processes and procedures change.

DRAFT – STEPS TO HIPAA COMPLIANCE

To support the tracking and reporting of state entity progress towards HIPAA compliance, the following standard definitions of project stages will be used by OHI:

- 1) **Project Initiation** (also called Awareness) needs to be established with executive level sanctioning of the efforts. Awareness can be established in a variety of ways: bringing in industry specialists, attending conferences, reviewing the federal rules and reading credible literature. This step will also help identify the main issues the program may have to address and to create an Initial Project Plan and tasks to establish compliance. In this step it is important to establish a Project Leader and Workgroup. In this first step, organizations need to begin participating in the Statewide HIPAA Workgroup and Sub-Workgroup to help coordinate and communicate issues and resolutions.
- 2) Conduct an **Initial Assessment** (also called an Inventory) to establish which programs and functions are impacted. This may require training staff and interactions with your business partners. This step will also identify **External Interfaces** that you will need to interact with as you implement any changes.
- 3) A **Project Plan** is established from the tasks initially identified for achieving compliance. The Plan will identify the main tasks and milestones for achieving compliance, designate staff for each task and establish dates for task completion. The Plan becomes a tool for monitoring progress and addressing issues as your project proceeds. The Plan also helps establish a detailed resource and cost estimate for the project. A more detailed Project Plan and resource - cost estimate can be established after the Gap Analysis is completed. Project Plans need to evolve as the project and resources change.
- 4) A **Detailed Assessment** (also called a Gap Analysis or Impact Assessment) should be performed on the programs and functions that require change. The Gap Analysis looks at the gaps between the current process and procedures compared to the Federal HIPAA rules. It will also investigate the options and desired tasks needed for achieving compliance to the rules.
- 5) **Implementation** (also called Remediation) is the final step. It involves making the changes to processes and procedures, revising user instructions, training staff, testing all changes, testing with your business partners, having a coordinated implementation process, and monitoring the new processes.

Variations of these steps may be needed for different organizations depending on the extent of changes and number of business partners involved. Critical throughout the process is top management involvement, monitoring progress toward goals, and communication and coordination with your business partners. With HIPAA being a series of Federal Rules being released and revised at periodic points, several of the above steps may need to be repeated as the rules change.